UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

JACOB DELANEY,

Defendant.

MEMORANDUM OF LAW
Filed Under Seal

O'CONNELL AND ARONOWITZ
Attorneys for Defendant
54 State Street
Albany NY 12207-2501
(518) 462-5601

SCOTT W. ISEMAN, ESQ.
Of Counsel

Dated: January 26, 2021

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Federal Cases

SUMMARY OF ARGUMENT

The search warrant application in this matter is deficient, in that, it utterly fails to establish probable cause and justify the requested search.

All evidence seized pursuant to this warrant must be suppressed because the warrant application relied upon a single alleged visit of an unknown duration to a website ("Target Site") seven and a half months earlier from an IP address that law enforcement can only identify as one of many possible IP addresses involved in the relay of information to and from the Target Site.

Additionally, the applying agent's own representations starkly contradict his conclusory assumption that evidence of criminality exists at the location identified in the application.

Furthermore, the Government's search and the resulting seizures cannot be saved by the good faith exception to the Exclusionary Rule since: the applying agent demonstrated gross negligence by ignoring clearly established Second Circuit search and seizure law; the application so lacked indicia of probable cause that it was unreasonable to rely upon it; and the applying agent recklessly provided misleading information to the reviewing magistrate by failing to include critical facts and making unsupported conclusions about the likelihood that evidence of criminality would be found at the location to be searched. As a consequence, all evidence obtained from the search of the Defendant's electronic devices and premises must be suppressed.

Likewise, any statements law enforcement obtained from the Defendant during and following the execution of this warrant should be suppressed.

Procedural Background and Factual Summary

The relevant procedural history and facts are recited in the accompanying attorney Declaration of Scott W. Iseman, Esq. and are incorporated here by reference.

Legal Standard

On a motion to suppress physical evidence, the Defendant bears the initial burden of proof. *United States v. Peeples*, 962 F.3d 677, 692 (2d Cir. 2020). But where, as here, the Defendant establishes a basis for the motion, the burden shifts to the Government. *United States v. Walker*, 922 F. Supp. 732, 750 (N.D.N.Y. 1996).

A valid warrant must be supported by probable cause and before a warrant can be issued, the reviewing magistrate must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates,* 462 U.S. 213, 238 (1983). A court reviewing the sufficiency of a warrant application "may conclude that a warrant is invalid where the magistrate's "probable-cause determination reflect[s] an improper analysis of the totality of circumstances." *United States v. Raymonda,* 780 F.3d 105 (2d. Cir. 2015) (*quoting United States v. Falso*, 844 F.3d 110, 117 (2d. Cir. 2008)) (internal quotation marks omitted). In addition, the Second Circuit has held that a warrant may lack probable cause "where the facts supporting criminal activity have grown stale by the time that the warrant issues." *Id*. citing *United States v. Wagner*, 989 F.2d 69 at 75 (2d Cir. 1993). The two critical factors in determining staleness are the age of the facts alleged and the "nature of the conduct alleged to have violated the law." *United States v. Ortiz,* 143 F.3d 728, 732 (2d Cir.1998)

The federal courts, and the Second Circuit in particular, have developed a specific probable cause sufficiency and staleness analysis in cases, like the instant matter, involving allegations of internet-based child pornography offenses. The Second Circuit's probable cause analysis in such cases focuses on whether there is evidence the targeted user has a predisposition for possessing or accessing contraband images. *Raymonda*, 780 F.3d at 115 ("evidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images—or

have obtained new ones—in the present." (internal citation and quotations omitted); s*ee also United States v. Irving*, 542 F.3d 110, 125 (2d Cir. 2006) (it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes").

The courts have inferred such a predisposition to avoid staleness and other probable cause sufficiency issues in circumstances where: the suspect admitted to possession, paid for or subscribed to services to receive contraband images; where the suspect has a prior history with child pornography, and even where the suspect downloaded and redistributed a single image. *Raymonda*, 780 F.3d at 114-15 (collecting cases). As the Second Circuit recognized in *Raymonda*, "[s]uch circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged." *Id*. But visiting a website or attempting to access a website where there may be contraband images is not a sufficient basis alone for probable cause. *Falso*, 844 F.3d at 121.

If a warrant was not supported by probable cause, preclusion does not automatically follow. Instead, the Government can attempt to rely on the good faith exception to the Exclusionary Rule. The good faith exception provides that evidence obtained in violation of the Fourth Amendment may still be used against a Defendant provided law enforcement applied for, obtained and objectively relied upon the search warrant in "good faith." *Raymonda*, 780 F.3d at 117-18; *Falso* 844 F.3d at 125.

The Exclusionary Rule does apply and suppression should follow, however, in instances where law enforcement exhibits "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *United States v. Stokes*, 733 F.3d 438, 443 (2d Cir. 2013). Similarly, once controlling precedent is set on what is legally required to establish probable cause, law

enforcement "may not thereafter claim reasonable reliance on warrants secured in the absence of compliance." *United States v. Clark*, 638 F.3d 89, 105 (2d Cir. 2011) (citing *United States v. Buck*, 813 F.2d 588, 592 (2d Cir. 1987)). The good faith exception also does not apply (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable. *United States v. Boles*, 914 F.3d 95, 103 (2d Cir. 2019).

While the Supreme Court has commented that most searches conducted pursuant to a subsequently invalidated warrant will ordinarily receive the benefit of the good faith exception, *United States v. Leon,* 468 U.S. 897, 922 (1984), it is the Government's burden to "demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." *Clark*, 638 F.3d at 100.

Statements made by a Defendant during and following an illegal search can also be suppressed as fruit of the poisonous tree. As a result, testimonial evidence derived from tainted evidence "up to the point at which the connection with the unlawful search becomes so attenuated as to dissipate the taint" should be suppressed under the Exclusionary Rule. *Murray v. United States*, 487 U.S. 533, 537 (1988). It is the Government's burden to prove that "the statements were sufficiently attenuated to remove the taint from the unlawful search." *United States v Guzman*, 724 F. Supp.2d 434, 444 (S.D.N.Y 2010) (*citing Mosby v. Senkowski*, 470 F.3d 515, 521 (2d. Cir 2006). A number of factors form the basis of an inquiry into whether the original taint of the illegal search has dissipated: "(1) the giving of Miranda warnings, (2) the "'temporal proximity'" of the illegal entry and the alleged consent, (3) "'the presence of intervening circumstances,'" and (4) the "'purpose and flagrancy of the official misconduct. '" *United States v. Snype*, 441 F.3d 119, 134

(2d Cir. 2006) (quoting *Kaupp v. Texas*, 538 U.S. 626, 633 (2003). In sum, the practical approach to the attenuation analysis is whether the causal link between the statements and the Fourth Amendment violation is "so long or tortuous that suppression of the evidence is unlikely to have the effect of deterring future violations of the same type." *Guzman*, 724 F. Supp. 2d at 444.

ARGUMENT

POINT I

There Is No Probable Cause Because the Warrant Application At Most identified the Defendant's IP Address As One of Many Potential IP Addresses Involved In A Relay of Computers Used By An Unidentifiable Party To Access the Target Site.

According to SA Fallon's application, the Target Site could only be accessed using the TOR network, which is a network of linked computers that masks a user's identity. Ex. "E" to Iseman Dec. at ¶ 9, 23. SA Fallon's application stated that TOR was designed to specifically facilitate anonymous internet communications through a distributed network of intermediary computers or relay nodes that are donated to the network by the network's users. *Id*. at ¶ 8. SA Fallon stated that "due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located." *Id*. at ¶ 19. According to SA Fallon, "[w]hen a TOR user accesses an Internet website, ***only the IP address of the last relay computer (the "exit node") as opposed to the TOR user's actual IP address***, appears on the website's IP log." *Id.* (emphasis supplied). Because of this structure, SA Fallon advised the court that "traditional IP address identification techniques are not effective." *Id*.at ¶ 8.[1]

[1] Although not included in the warrant application, SA Fallon's understanding of the TOR network is corroborated in the investigatory lead information sent to the FBI's Albany Division about this case, which stated that because of the TOR network's structure, "[c]urrently, there is no practical method to trace a user's actual IP address back through those Tor relay computers." Ex. "D" to Iseman Dec. at pg. 3.

Despite stating that there is no way to differentiate the actual TOR user's IP address from the other relay nodes in the network, SA Fallon represented to the court that there is a "link" between the Target Website, its contraband and the Defendant's IP address. *Id*. at ¶ 6. Inexplicably, however, SA Fallon never resolves the threshold problem he identifies in his application – that when a TOR browser is used, law enforcement cannot determine the TOR user's IP address. *Id.* at ¶¶ 8, 11. SA Fallon never explains how either the FBI or the FLA determined that the Defendant's IP address was the user who accessed the Target Site rather than some intermediary relay or the last exit node in that relay. The most SA Fallon stated is that the FLA "determined" the Defendant's IP address accessed the Target Site. *Id*. at ¶ 20. But he does not describe ***how*** that determination was made except through some undescribed "independent investigation" overseas. [2] *Id*. at ¶ 21. In fact, based on the information provided by SA Fallon, the only logical conclusion that he could make based on the information he received from the FLA and his stated training and experience was that the Defendant's IP address is the exit node ***and not the actual user*** who accessed the Target Site. *Id*. at ¶ 11

Without resolving this glaring issue, the most the Government could have represented to the court is that the Defendant's IP address was either the exit node or one of an unknown number of intermediary relay computers that were used to access the Target Site on April 22, 2019. Even if the Government had only made that representation, however, it would have to concede that if the Defendant's IP address was the last exit node or an intermediary relay, a user at the Defendant's

[2] The FLA represented that it did not do anything on United States' soil and did not violate any of its own laws to obtain the information it referred to the Government. The FLA never explained to the Government how it obtained the IP address information. *See* Ex. "B" to Iseman Dec. And there is no indication that the Government asked the FLA about how it identified the Defendant's IP address – a question called for in light of the FBI's admission that "there is no practical method to trace a user's actual IP address back through those Tor relay computers." Ex. "D" to Iseman Dec. at pg. 3.

IP address would not be able to see or access the content passing through the computer as part of the relay because such transmissions are encrypted, preventing anyone in the relay except the actual user from accessing the content. *Id*. As a result, even if the Defendant's IP address was "linked" to the Target Site through the TOR relay, as an intermediary or exit relay, a user at the Defendant's IP address would not be able to see or access any contraband content that may pass through that relay.

For the simple reason that the search warrant application at no time explains how SA Fallon, the Government, or the FLA differentiated the Defendant's IP address from the IP addresses used in the TOR network relay, including the last exit node, the Government did not have probable cause to obtain its warrant. This error demonstrates the warrant application was so clearly lacking in indicia of probable cause as to render the Government's reliance upon it unreasonable. *Boles*, 914 F.3d at 103. As a result, suppression of all seized evidence is the only available remedy.

POINT II

The facts underlying the warrant application are independently deficient and stale.

The probable cause analysis for this case can be taken nearly verbatim out of the Second Circuit's decisions in *Falso* and *Raymonda*. And because *Falso* and *Raymonda* are clearly established Second Circuit authority, law enforcement does not get a good faith mulligan when their conduct runs afoul of these clear holdings. *Clark*, 638 F.3d at 105 (citing *United States v. Buck*, 813 F.2d at 592 (2d Cir. 1987). Like in *Falso* and *Raymonda*, the Government's application here was supported by only ***one*** alleged instance of accessing a site affiliated with contraband images and provided no additional information from which a reviewing magistrate could infer that

the targeted user had a predisposition toward child pornography. Not only were the supporting facts clearly deficient, but they were also obviously too stale to form a basis for probable cause.

Specifically, SA Fallon applied for the warrant seven months and eighteen days (or 238 days) after the ***only alleged instance*** of the Target Site being accessed for an ***unstated duration***. *Cf Raymonda*, 780 F.3d at 117 (no probable cause in part because of nine-month gap between single access and warrant execution). Additionally, while the application states that the Target Site's users needed to register for an account to access the vast majority of the contraband material (Ex. "E" to Iseman Dec. at ¶ 20), SA Fallon provided no evidence that the Defendant or a user from the Defendant's IP address was a registered user or logged into a preexisting account on April 22, 2019 or at any other time. Likewise, although SA Fallon described that detailed data about an individual user and their activity on the Target Site like the "date a user joined, total posts, most active forum and most active topic" is available simply by clicking on the user's name, no such information related to these data points is provided in the application regarding the targeted user or the Defendant. Ex. "E" to Iseman Dec. at ¶ 16. There is also no evidence that the targeted user or the Defendant saved any illicit images or even accessed or viewed the specific contraband images described in ¶ 18 of the application as being trafficked through the site. *Id*. at ¶ 18. Furthermore, there is no indication that the Government ever attempted to follow up with the FLA regarding these issues.

Similarly, while the application states that "users were able to view some material without creating an account", "some material" is never described or defined. *Id*. at ¶ 20. While the application incorporated verbatim the FLA's statement that the Defendant or Defendant's IP address "accessed online child sexual abuse material via the Target Site", "online child sexual abuse material" is not defined by the FLA or SA Fallon. *Cf Id.* at ¶ 20 and definitions provided in

¶ 5. Importantly, SA Fallon does define "child pornography", "child erotica", "sexually explicit conduct", and "visual depiction" but he never defines or identifies "online child sexual abuse material" as child pornography, child erotica, sexually explicit conduct or any kind of contraband, despite carefully establishing those definitions and his experience with the same at the outset of the application. *Id*. at ¶5(d), (e) and (p). Moreover, there is no information provided about what that phrase means under the FLA's country's laws. In fact, the "online sexual abuse material" described by the FLA may merely be text regarding the Target Site and available content as opposed to actual contraband images or videos. Since SA Fallon does not say one way or another, the reviewing court could not know. Because of the failure to particularize and define, this Court cannot conclude or infer that the material the FLA referred to was actually contraband, when broad terms like "material" used by a foreign entity could mean a host of things that is not indicative of criminal conduct.

Furthermore, the application provides no evidence that the Defendant or anyone associated with the Defendant's IP address had a propensity for collecting child pornography. Beyond boilerplate information about child pornography cases involving the internet and computers, the application attempts to suggest that it can be inferred that the target is a child pornography collector because SA Fallon learned from other agents in a ***different*** case involving a ***different*** TOR-based child pornography site, that it was "exceedingly rare for a registered site user to access that site and never return." *Id*. at ¶ 22. But again, there is no evidence or suggestion that the Defendant or anyone affiliated with the Defendant's IP address was a registered user of the Target Site.

The most the Government can argue in this respect is that a TOR browser was required to access the Target Site and the Target Site is not as easy to find online as "websites that operate on the open internet." *Id*. at ¶ 23. But those factors, without more, are not enough to establish

"propensity-raising circumstances" that the Defendant or a user at the Defendant's IP address collected child pornography. *Raymonda*, 780 F.3d at 116. Some additional indicia beyond the use of a privacy program and being part of a relay chain of other TOR users involved in accessing a website where contraband may be available must be required to conduct the requested search. *Falso*, 544 F.3d at 124 ("Generalized allegations about: (1) the propensity of collectors of child pornography to intentionally maintain illegal images; (2) law enforcement's ability to retrieve such images from a computer; and (3) the ability to view child pornography on the [subject]website, fail to establish the requisite nexus of illegal activity to [the targeted user]"). This must be especially true where, as here, no evidence was presented that the Defendant's IP address was a registered user of the Target Site, logged in, requested, shared, purchased, redistributed, clicked on or downloaded any purported contraband. *Raymonda*, 780 F.3d at 116.

As such, even assuming the Defendant's IP address was the actual TOR user, there are no factors to "negate the possibility that [the Defendant's alleged] brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged." *Raymonda*, 780 F.3d at 115. Importantly, the Target Site ceased operating in June 2019 ('Ex. "E" to Iseman Dec. at ¶ 15), meaning that whoever accessed the Target Site on April 22, 2019, had approximately only two more months to access the Target Site again, thereby reducing the likelihood of revisiting and increasing the likelihood that the "residue" of any past encounter was "long ago expunged" by the time law enforcement executed the search six months after the Target Site shut down. *Raymonda*, 780 F.3d at 115. Therefore, like in *Falso* and *Raymonda*, there was clearly insufficient evidence to establish probable cause to issue the subject warrant.

POINT III

The Good Faith Exception Does Not Save the Government's Search and Resulting Seizure

The Government has the burden to "demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." *Clark*, 638 F.3d at 100 (citation and quotation marks omitted). But the Government cannot "claim reasonable reliance on warrants secured in the absence of compliance" with established legal precedent. *Id*. at 105. As described above, since *Falso* and *Raymonda* are clearly established controlling precedent and the same probable cause errors are repeated here, the Government does not get the benefit of the good faith exception.

But even if this court finds a way to distinguish *Falso* and *Raymonda*, the good faith exception would still not apply because the application was so grossly deficient that the Government could not objectively rely on the warrant. *Boles*, 914 F.3d at 103. As described above, the application failed to explain how the Defendant's IP address was determined to be that of the TOR user who allegedly accessed the Target Site when TOR frustrates law enforcement's ability to trace IP information to identify the actual TOR user. Ex. "E" to Iseman Dec. at ¶ 8. Moreover, the information's staleness and lack of any affirmative conduct by the Defendant or a user allegedly affiliated with Defendant's IP address that demonstrates a predisposition for collecting child pornography, all add up to a grossly deficient application that could not be relied upon in good faith.

Additionally, SA Fallon, at the very least, recklessly mislead the magistrate with his application, which is an independent basis for denying the good faith exception. *Boles*, 914 F.3d 103 (2d Cir. 2019) (good faith exception does not apply where agent knowingly misleads magistrate); *Raymonda*, 780 F.3d at 118 (recklessly seeking a warrant prohibits good faith

exception) (citations omitted). Because of the glaring deficiencies pointed out above, SA Fallon, made baseless, conclusory representations that there was probable cause to search the Defendant's residence and electronic devices. Relatedly, SA Fallon made it appear as though the user of the Defendant's IP address had registered for an account with the Target Site, by providing detailed descriptions of what a user ***could do*** once logged in (Ex. "E" to Iseman Dec. at ¶ 17), the user data that is available (*Id*. at ¶16), and even listing the specific identifiable contraband images that were trafficked through the site once logged on. *Id*. at ¶18. But again, there is no evidence the Defendant or a user at the Defendant's IP address had a registered account, ever logged into the Target Site or accessed the described images. Indeed, this was no "good faith" omission since no such registration evidence was apparently produced to the FBI by the FLA and the FBI apparently never followed up with the FLA by asking for any such information. "Ex. "B" and "D" to Iseman Dec.

Similarly, SA Fallon stated at the outset of the application that a

> user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography…there is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE as further described herein.

Ex. "E" to Iseman Dec. at ¶ 6. Representing such a link, without actually providing it, due, again, to not solving the threshold IP address identification issue, is a gross overstatement. Particularly since SA Fallon and the Government had opposite, contradictory and exculpatory information regarding the Defendant and the Defendant's IP address but failed to include that information in its application. *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.), *on reh'g*, 91 F.3d 331 (2d Cir. 1996) (good faith exception "does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge"); *United States v. Ganias,* 824 F.3d 199, 221 (2d Cir. 2016) ("to assert good faith reliance successfully, officers must, *inter alia*, disclose all

potentially adverse information to the issuing judge"). For example, prior to applying for the warrant, the FBI determined that the Defendant's IP address was not registered with the National Center For Missing and Exploited Children ("NCMEC") or the ICAC Child Online Protection System. "Ex. "D" to Iseman Dec. at pg. 4. It was also determined that the Defendant had no prior criminal history, was not a registered sex offender, and FBI database searches "did not identify any derogatory information" about the Defendant. *Id*. at pg. 5. None of this was made known to the court.

SA Fallon also included pages of boilerplate information about child pornography cases, predilections of past offenders and use of the internet and the Tor program that have ***nothing to do with the Defendant*** or his IP address. These types of boiler plate generalizations are dangerously misleading. As Judge Chin noted in his separate opinion in *Raymonda*: it is "inappropriate-and heedlessly indifferent" for an agent to "rely on boilerplate language regarding the proclivities of collectors" when there is no evidence that the Defendant or the Defendant's IP address are actually involved in the collection of child pornography. 780 F.3d 105, 124 (2d Cir. 2015), (Chin, J. concurring in part and dissenting in part).

While these gross generalizations and omissions should trouble the court, there is more. Importantly, the lead that was sent to the FBI's Albany Division that triggered this investigation, expressly stated "there is no practical method to trace a user's actual IP address back through those Tor relay computers." Ex. "D" to Iseman Dec. at 3. Perhaps in recognition that the FBI could not identify who the actual Tor user was who accessed the Target Site, the referring agent provided the Albany Division with a draft affidavit for a pen register/trap and trace pony ("PRTT") and stated that a "PRTT can be effective in determining whether the Tor network traffic is coming from a residence." *Id*. at 6. Perhaps the PRTT could have provided some insight into whether TOR

activity was still occurring at the Subject Premises months after the alleged Target Site was accessed. But the Government never applied for a PRTT application and never referred to this fact in its application.

Since the application falls well short of probable cause standards set in *Falso* and *Raymonda*, the facts provided were stale and grossly deficient, and since it is never explained how the Defendant's IP address was identified as the TOR user's rather than the exit node or one of many in the relay, the Government cannot be given the benefit of the good faith exception. To decide otherwise blesses grossly negligent and reckless law enforcement conduct – exactly the conduct the Exclusionary Rule is supposed to deter. *Herring v. United States,* 555 U.S. 135, 144 (2009) (The exclusionary rule serves to deter "deliberate, reckless, or grossly negligent conduct."). Thus, there cannot be a finding of good faith here.

POINT IV

The Defendant's Statements Should be Suppressed.

All statements the Defendant made on December 12, 2019 should also be suppressed as they are the product of the Government's unlawful search and seizure and are not attenuated in time or place to the Fourth Amendment violation. *Murray v. United States*, 487 U.S. 533, 537 (1988). The Government cannot prove that any of the Defendant's statements, even those that followed *Miranda* warnings, are "sufficiently attenuated to remove the taint from the unlawful search." *United States v. Guzman*, 724 F. Supp. 2d 434, 444 (S.D.N.Y 2010).

Furthermore, each factor the Court is instructed to consider when evaluating attenuation, *see United States v. Snype*, 441 F.3d 119, 134 (2d Cir. 2006), with the exception of an eventual *Miranda* advisement, tips in favor of suppression since the statements were made either on scene or immediately following execution of the warrant. Ex. "I" to Iseman Dec. at pgs. 1-3.

Additionally, the post-*Miranda* statements were guided by ongoing analysis and review of the Defendant's electronic devices, which directly connects his post-*Miranda* statements to the illegal search. *Id*. Finally, there is no intervening event or temporal break that establishes that these statements were freely given to the Government. *United States v. Seldinas*, 2014 WL 6669901, *7 (W.D.N.Y.2014) ("[o]nce a defendant thinks that he has been caught red handed, the futility of remaining silent can be more easily exploited by law enforcement ... because the realization that the cat is out of the bag plays a significant role in encouraging the suspect to speak") (quoting *United States v. Griswold*, 2011 WL 7473466, *11 (W.D.N.Y.2011)) (internal quotation omitted). As a result, all of the Defendant's statements from December 12, 2019 to law enforcement must be suppressed.

CONCLUSION

For the above reasons, the Defendant respectfully requests that the Court suppress all evidence seized during the search of the Defendant's apartment and any statement made by Defendant to law enforcement on December 12, 2019.

Dated: Albany, New York
January 26, 2021

O'CONNELL & ARONOWITZ P.C.

By: 

Scott W. Iseman Esq.
Attorney for Plaintiff
Bar Roll No.: 518859
54 State Street, 9th Floor
Albany, NY 12207
(518) 462-5601
siseman@oalaw.com